

Anti-DDoS Advanced Operation Guide Product Documentation





Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

STencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Operation Guide

Operation Overview

Protection Overview

Use Limits

Protection Configuration

DDoS protection

- Protection Level and Cleansing Threshold
- Protocol Blocking
- Watermark Protection
- Feature Filtering
- **AI Protection**
- IP Blocklist/Allowlist
- Port Filtering
- **Regional Blocking**
- IP and Port Rate Limiting
- **Connection Attack Protection**
- CC protection
 - Protection Level and Cleansing Threshold
 - Intelligent CC Protection
 - **Precise Protection**
 - CC Frequency Limit
 - **Regional Blocking**
 - IP Blocklist/Allowlist

Business Connection

- Port Connection
- Domain Name Connection
- **Configuring Session Persistence**

Instance Management

- Viewing Instance Information
- Setting Instance Alias and Tag
- Configuring Intelligent Scheduling
- Setting Security Event Notification
- **Viewing Operation Log**
- **Blocking Operations**
 - Connecting a Blocked Server



Unblocking an IP

Operation Guide Operation Overview

Last updated : 2022-07-06 17:08:59

This document lists the references for common operations in Anti-DDoS Advanced.

Reference

- Viewing security protection overview
- Use Limits

Protection Configuration

DDoS protection

- Protection Level and Cleansing Threshold
- Protocol blocking
- Watermark protection
- Attribute Filtering
- Al protection
- IP blocklist/allowlist
- Port Filtering
- Regional Blocking
- IP and Port Rate Limiting
- Connection Attack Protection

CC protection

- Protection level and cleansing threshold
- Targeted protection
- CC frequency control
- Regional Blocking
- IP Blocklist/Allowlist

Business Connection

- Port connection
- Domain name connection
- Configuring session persistence
- Configuring health check

Instance Management

- Viewing instance information
- Setting instance alias and tag
- Modifying elastic protection bandwidth

Scheduling and Unblocking

Configuring intelligent scheduling

Operation Log

Viewing operation log

Blocking Operations

Unblocking an IP

Protection Overview

Last updated : 2022-06-10 14:10:15

Protection Overview

The protection overview page of the Anti-DDoS console shows you complete, real-time indicators for basic protection, Anti-DDoS Pro, and Anti-DDoS Advanced applications, including the protection status and DDoS attack events, which can be used for analysis and source tracing.

Viewing attack statistics

1. Log in to the new Anti-DDoS console, and select **Overview** on the left sidebar to enter the **Protection Overview** page.

Anti-DDoS	Overview						
🔛 Overview	Protection Overview	Anti-DDoS Basic	Anti-DDoS Pro	Anti-DDoS Advanced			
Anti-DDoS Basic	Attacks						
Anti-DDoS ~ Advanced					Attacked IPs	Protected IPs	Blocked IPs
다 Anti-DDoS Pro 👻				Safe	0	50	0
 Intelligent * Scheduling Policy 				No abnormal traffic detected.	Attacked domain names	Protected domain names	Peak attack bandwidth
Ø Anti-DDoS Pro					0	30	O Mbps

- 2. In the "Attacks" module, you can view the application security status, the latest attack and the attack type. To obtain higher protection, you can click **Upgrade Protection**.
- 3. This module also displays the details of the following data.



Field description:

 Attacked IPs: The total number of attacked application IPs of basic protection, Anti-DDoS Pro and Anti-DDoS Advanced.

- Protected IPs: The total number of protected application IPs of Anti-DDoS Pro and Anti-DDoS Advanced.
- Blocked IPs: The total number of blocked IPs of basic protection, Anti-DDoS Pro and Anti-DDoS Advanced.
- Attacked domain names: The total number of domain names of attacked Anti-DDoS Advanced instances and ports.
- Protected domain names: The number of domain names connected to Anti-DDoS Advanced instances.
- Peak attack bandwidth: The maximum attack bandwidth of the current attack events.

Viewing defense statistics

- 1. Log in to the new Anti-DDoS console, and select **Overview** on the left sidebar to enter the **Protection Overview** page.
- 2. In the "Defense" module, you can easily see the application IP security status.



Field description:

- Total IPs: The total number of application IPs, including IPs of basic protection, Anti-DDoS Pro and Anti-DDoS Advanced.
- Protected IPs: The total number of protected application IPs of Anti-DDoS Pro and Anti-DDoS Advanced.
- Blocked IPs: The total number of blocked IPs of basic protection, Anti-DDoS Pro and Anti-DDoS Advanced.
- 3. This module also displays the total number of attacks on your applications, giving you a picture of the distribution of attacks.





4. Meanwhile, this module provides recommended actions for the attacked IPs connected to basic protection, allowing you to quickly upgrade your Anti-DDoS service.

Recommended Actions	
Upgrade Anti-DDoS for	Anti-DDoS Pro Anti-DDoS Advanced

Viewing Anti-DDoS Advanced instance statistics

- 1. Log in to the new Anti-DDoS console, and select **Overview** on the left sidebar to enter the **Protection Overview** page.
- 2. The "Anti-DDoS Instances" module visualizes the Anti-DDoS instance status data, providing an easy and complete way to know the distribution of insecure applications.

ti-DDoS Instances					
	Running	15		Running	37
Service Packs	Blocked	0	Anti-DDoS Advanced	Blocked	0
CI	Being attacked	0	41	Being attacked	з
	Other	o		Other	1

Viewing recent events

- 1. Log in to the new Anti-DDoS console, and select **Overview** on the left sidebar to enter the **Protection Overview** page.
- 2. The "Recent Events" module shows you all the recent attack events. For attack analysis and source tracing, click **View Details** to enter the event details page.

Recent Events							
Attacked IP	Instance Name	Defense Type 🔻	Start Time	Duration	Attack Status 🔻	Event Type T	Operation
	All second se	Anti-DD 1	2022-02-16 04:07:00	2 mins	Attack ends	DDoS Attack	View Details
		Anti-DDo1	2022-02-14 17:35:00	2 mins	Attack ends	DDoS Attack	View Details
11.	10 A second	Anti-DDoS	2022-02-13 12:05:00	2 mins	Attack ends	DDoS Attack	View Details

3. In the "Attack Information" module of the event details page, you can view the detailed attack information for the selected period, including the attacked IP, status, attack type (which is sampled data), peak attack bandwidth and attack packet rate, and attack start and end time.

DDoS Atta	ck Details			
Attack Info	ormation			
Attacked IP	11	Attack Bandwidth Peak	OMbps	
Status	Attack ends	Attack packet rate peak	730pps	
Attack Type	SYNFLOOD	Attack start time	2022-02-16 04:07:00	
		Attack end time	2022-02-16 04:09:00	

4. In the "Attack Trend" module of the event details page, you can view the trend of attack bandwidth and attack packet rate and easily find the peak spikes.

Note :

This module provides complete, real-time data in the attack period.



Attack Bandwidth	Attack Packet Rate
10 Mbps	
8 Mbps	
6 Mbps	
4 Mbps	
2 Mbps	
2022-02-16 04:00	2022-02-16 04:

5. In the "Attack Statistics" module of the event details page, you can view how attacks distribute over different attack traffic protocols and attack types.





Field description:

- Attack traffic protocol distribution: It displays how attacks on the selected Anti-DDoS Advanced instance distribute over different attack traffic protocols within the queried period.
- Attack type distribution: It displays how attacks on the selected Anti-DDoS Advanced instance distribute over different attack types within the queried period.
- 6. The "Top 5" modules of the event details page displays the top 5 attacker IP addresses and the top 5 attacker regions, which is helpful to precise protection configuration.



Note :

This module provides sampled data in the attack period.

Top 5 Attacking Source IPs		Top 5 Districts Where Attacks Originate	
62.197.136.161	256	Netherlands	512
89.248.163.136	256		

7. In the "Attacker Information" module of the event details page, you can view the sampled data of the attack period, including the attacker IP, region, total attack traffic, and total attack packets.

Note:

This module provides sampled data in the attack period.

Attack source information

Attack Source IP	Region	Cumulative attack traffic	Cumulative attack volume
62.1	Netherlands	16.0 MB	256
89.	Netherlands	16.0 MB	256
Total items: 2		N N	1 / 1 page 🕨 🕨

Anti-DDoS Advanced Overview

After an IP address is bound to an Anti-DDoS Advanced instance, when you receive a DDoS attack alarm message or notice any issue with your business, you need to view the attack details in the console, including the attack traffic and current protection effect. Enough information is critical for you to take measures to keep your business running smoothly.



S All Regions - S All Lines - Please select

Viewing DDoS protection details

1. Log in to the new Anti-DDoS console, select **Overview** on the left sidebar and then open the **Anti-DDoS Advanced** tab.

My usage 0 0 0 Blocked 0 0 Blocked 0 Blocked 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	My Anti-DDoS Advanced instances	Protecting	Ŀ	Blocked DDoS attacks
• Activated 0 • 0 Blocked CC attacks Renew Now Blocked CC attacks O times	My usage	0 Being attacked 0 Blocked		U times
	• Activated 0 • 0 Renew Now	0	Ð	Blocked CC attacks 0 times

2. On the **DDoS Attack** tab, select a query period, target region, and an instance to check whether the instance has been attacked. The complete attack data is displayed by default.

Note : You can query attack traffic and DDoS attack events in the past 180 days.
DoS Attack CC Attack

2. View the information of attacks suffered by the selected Anti-DDoS Advanced instance within the queried period, such as the trends of attack traffic bandwidth and attack packet rate.

Last 6 Hours

Today

Last 7 Days

Last 15 days

Last 30 Days

Last 1 Hour

S All Regions * S All Lines * Please select	et 👻 Last 1 Hour Last 6 Hours	Today Last 7 Days	Last 15 days Last 30 Days 2022-02-17 16:30 ~ 2022-02-17 17:30	
Attack Traffic Bandwidth (traffic surges in	cluded)	Attack Bandwidth Peak	Attack Packet Rate	Attack packet rate peak 0 pps
10 Mbps			10 pps	
8 Mbps	2022-02-17 16:45		8 pps	
6 Mbps	- 0 Mbps		6 pps	
4 Mbps			4 pps	
2 Mbps			2 pps	
2022-02-17 16:30 2022-02-1	7 1645 2022-02-17 17:00 2022-02-17 17:15	2022-02-17 17:30	2022-02-17 1630 2022-02-17 1645 2022-02-17 17:00 2022-02-17 17:15	2022-02-17 17:30

3. You can view the recent DDoS attacks in the **Recent Events** section. To view details of an event, you can click **View Details**. To view sampled attack data within a period, click **Packet Download**.

• View Details: You can view information including attacker IP, attack source region, generated attack traffic, and attack packet size, providing support for your source analysis and tracing.

2022-02-17 16:30 ~ 2022-02-17 17:30

Ē.

DDoS Attack Details					
Attack Info	ormation				
Attacked IP	11	Attack Bandwidth Peak	0Mbps		
Status	Attack ends	Attack packet rate peak	730pps		
Attack Type	SYNFLOOD	Attack start time	2022-02-16 04:07:00		
		Attack end time	2022-02-16 04:09:00		

• Packet Download: The sampled attack packet data can be downloaded to help customize a protection plan.

tack Packet List		:
ID	Time	Operation
12993844	2022-01-10 23:37:51	Download
12993866	2022-01-10 23:37:51	Download
Total items: 2	10 🔻 / page 🛛 🖌 🖣	1 / 1 page 🕨 🕨

4. In the **Attack Statistics** section, you can view how the attacks distribute across different attack traffic protocols, attack packet protocols, and attack types.



Field description:

- Attack traffic protocol distribution: It displays how attacks on the selected Anti-DDoS Advanced instance distribute over different attack traffic protocols within the queried period.
- Attack packet protocol distribution: It displays how the attacks suffered by the selected Anti-DDoS Advanced instance distribute across different attack packet protocols within the queried period.
- Attack type distribution: It displays how attacks on the selected Anti-DDoS Advanced instance distribute over different attack types within the queried period.
- 5. In the attack source section, you can view the distribution of DDoS attack sources in and outside the Chinese mainland within the queried period, so that you can take further protective measures.



Viewing CC protection details

1. On the **CC Protection** tab, select a query period, target region, and an instance to check whether the instance has been attacked.

DDoS Attack	CC Attack									
S All Regions 🔻	Please select	Ŧ	Last 1 Hour	Last 6 Hours	Today	Last 7 Days	Last 15 days	Last 30 Days	2021-11-01 00:00 ~ 2022-02-17 23:59	Ö

2. You can select **Today** to view the following data to identify the impact of attacks on your business.

S All Regions * S All Lines * Please select	Last 1 Hour Last 6 Hours Today	Last 7 Days Last 15 days	Last 30 Days 2022-01-18 00:00 ~ 20	122-02-17 23:59	
CC Attack Trend Unit: qps	Attack Request	ak CC Attack Tren Unit: Times	nd		Total Request Peak 4422201 times
10,000 8,000 4,000 2,000		5,000,000 4,000,000 3,000,000 2,000,000 1,000,000	1		
2022-01-16 00:00 2022-01-24 00:00 2022-01-30 00:00 — Total request rate — Atta	2022-02-05 00:00 2022-02-11 00:00 2022 :k request rate	2-17 00:00 2022-01-18 0	0:00 2022-01-24 00:00	2022-01-30 00:00 20; — Total requests — Attack requ	22-02-05 00:00 2022-02-11 00:00 2022-02-17 00: uests

Field description:

- Total request rate: The rate of total traffic (in QPS).
- Attack request rate: The rate of attack traffic (in QPS).
- Total requests: The total number of requests received.
- Attack requests: The number of attack requests received.
- 3. You can view recent CC attacks in the **Recent Events** section. Click **View Details** on the right of an event to display the attack start and end time, attacked domain name, attacked URI, total request peak, attack request peak, and attacker IP. You can also check the attack information, attack trends, and detailed CC records.

Recent Events								
Instance ID	Attacked Domain Name	Attacked URI	Attacked IP	Attack Source	Start Time	Duration	Attack Status 🔻	Operation
bgpi		-			2022-02-17 15:51:00	1 mins	Attack ends	View Details
bgpi		-			2022-02-17 13:37:00	1 mins	Attack ends	View Details
bgi		-	1000		2022-02-17 12:41:00	1 mins	Attack ends	View Details

Viewing User Traffic Details

- 1. Log in to the new Anti-DDoS console. Select Anti-DDoS Advanced > Application Traffic on the left sidebar.
- 2. Select a query period, target region, and an instance to check whether the instance has been attacked. The complete DDoS attack data is displayed by default.

Note: You ca	n query traffic	c usage a	and DDoS at	tack events i	in the past 18	0 days.	
Last 1 Hour	Last 6 Hours	Today Please s	Last 7 Days	Last 15 days	Last 30 Days	2022-04-28 13:15 ~ 2022-04-28 14:15 •	t ¢

3. You can view the trends of inbound/outbound traffic, bandwidth and packet rate, as well as the number of active connections and new connections within the selected time period. The maximum bandwidth, connections and QPS can also be checked.

- Active connections: The number of TCP connections that are already established and currently active.
- New connections: The number of TCP connections that are newly established per second for communication between the client and the instance.

Use Limits

Last updated : 2023-05-09 16:59:58

Scenario

We recommended that you use Anti-DDoS Advanced to protect business IP addresses or domain names for website (layer-7) and non-website (layer-4) businesses in and outside Tencent Cloud.

Capability

By default, one Anti-DDoS Advanced instance supports a total of 60 forwarding rules for layer-4 access and layer-7 access. An Anti-DDoS Advanced instance supports 500 forwarding rules at most. For non-website (layer-4) protocols, each rule supports 20 source IP addresses or domain names. For website (layer-7) protocols, each rule supports 16 source IP addresses or domain names.

Note:

The total number of forwarding rules is the sum of forwarding rules for TCP/UDP and HTTP/HTTPS, and the maximum total number can be up to 500. For TCP and UDP, if the same forwarding port number is used, two different forwarding rules need to be configured.

Blacklist/Whitelist

- For DDoS protection, up to 100 IP addresses can be added to the blacklist and the whitelist in total.
- A URL allowlist is not supported.

Available Regions

At present, Anti-DDoS Advanced is available both in and outside Chinese Mainland. Specifically, it is supported in the following regions outside Chinese Mainland: Hong Kong (China), Taiwan (China), Singapore, Seoul, Tokyo, Virginia, Silicon Valley, and Frankfurt.

Protection Configuration DDoS protection Protection Level and Cleansing Threshold

Last updated : 2022-04-01 09:42:59

This document introduces the use cases of different protection levels and the actions Anti-DDoS Advanced takes to defend against DDoS attacks. You can follow this guide to set the DDoS protection levels in the console.

Use Cases

Anti-DDoS Advanced provides three available protection levels for you to adjust protection policies against different DDoS attacks. The details are as follows:

Protection Level	Protection Action	Description
Loose	 Filters SYN and ACK data packets with explicit attack attributes. Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specifications. Filters UDP data packets with explicit attack attributes. 	 This cleansing policy is loose and only defends against explicit attack packets. We recommend choosing this protection level when normal requests are blocked. Complex attack packets may pass through the security system.
Medium	 Filters SYN and ACK data packets with explicit attack attributes. Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specifications. Filters UDP data packets with explicit attack attributes. Filters common UDP-based attack packets. Actively verifies the source IPs of some access attempts. 	 This cleansing policy is suitable for most businesses and capable of defending against common attacks. The level Medium is chosen by default.

 packets that are not compliant with the protocol specifications. Filters UDP data packets with explicit attack attributes. Filters common UDP-based attack packets. Actively verifies the source IPs of some access attempts. Filters ICMP attack packets. Filters common UDP attack data packets. Strictly checks UDP data packets. 	Strict • Filters SYN and ACK data This cleansing packets with explicit attack this level when attributes. system on Nor • Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specifications. • Filters UDP data packets with explicit attack attributes. • Filters common UDP-based attack packets. • Actively verifies the source IPs of	attack packets pass through the security mal mode.
--	---	--

Note:

- If you need to use UDP in your business, please contact sales to customize an ideal policy for not letting the level Strict affect normal business process.
- The level Medium is chosen by default in each Anti-DDoS Advanced instance, and you can adjust the protection level as needed. Also, you can set the cleansing threshold, so that the traffic exceeding the set value can be automatically cleansed.

Prerequisites

You have successfully purchased an Anti-DDoS Advanced instance and set the protected target.

Directions

- 1. Log in to the DDoS console and click Anti-DDoS Advanced (New) -> Configurations on the left sidebar.
- 2. Select an Anti-DDoS Advanced ID or port from the left list, e.g., 212.64.xx.xx bgpip-000002jt

or 119.28.xx.xx bgpip-000002ju -> tcp:8000.

3. Choose a protection level and set the cleansing threshold in the DDoS Protection Level section.

Configuration Parameters

Protection Level

For each Anti-DDoS Advanced instance with the protection enabled, the level Medium is chosen by default and you can adjust the protection level as needed.

Cleansing Threshold

- It refers to the threshold to trigger cleansing. If the traffic is below the threshold, the cleansing action will not be taken even if attacks are detected.
- For each Anti-DDoS Advanced instance with the protection enabled, the cleansing threshold has a default value, and you can set the cleansing threshold as needed. The system will learn the change patterns of business traffic to generate a baseline.

Note :

If you have a clear concept about the threshold, set it as needed. Otherwise please leave it to the default value. Anti-DDoS will automatically learn through AI algorithms and generate the default threshold for you.

Protocol Blocking

Last updated : 2023-04-28 16:48:50

Anti-DDoS supports blocking the source traffic accessing Anti-DDoS instances based on specified protocols, such as ICMP, TCP, UDP, and other protocols. After the configuration is completed, all matched access requests will be directly blocked. Due to the connectionless feature of UDP protocol (unlike TCP, which requires a three-way handshake process), it has natural security vulnerabilities. If you do not have UDP businesses, we recommend blocking the UDP protocol.

Prerequisites

• You have purchased an Anti-DDoS Advanced instance and set the target to protect.

Directions

- Log in to the Anti-DDoS console and select Anti-DDoS Advanced (New) > Configurations on the left sidebar.
 Open the DDoS Protection tab.
- 2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxxx".

IP ▼ Q	IP/Port Protection Domain name protection
	 DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks In Loose Mode, only confirmed attack messages are blocked. In Medium me blocked. If attack messages failed to be blocked in the Strict mode, or the n Strict Medium Loose

3. Click Set in the "Protocol blocking" section.

IP Blocklist/Allowlist Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.	Port Filtering Block or allow traffic to an Anti-DDoS Advanced IP by specifying the source and destination port range
Configured 4 blocklists, 1 allowlists Set	Configured 1 rules Set
Block by protocol Block requests of the specified protocol according to the traffic to Anti-DDoS. If your application does not use UDP, it's recommended to block all UDP requests.	Watermark Protection Image: State of the symplection of the symplection of the symplection of the symplection of the symplectic symplecti symplectic symplecti symplectic symplectic symplectic sy
Configured 1 rules Set	Enabled 1 rules Set

4. Click Create.

Note:

The **Create** button appears only when you use this feature for the first time.



5. In the pop-up window, click the button on the right of a protocol, and click **Confirm**.



6. After the rule is created, it is added to the list. You can click **Configuration** on the right of the rule to modify it.

Block by protocol						
Create					Enter IP	Q
Associated Resource	Block ICMP Protocol	Block TCP Protocol	Block UDP Protocol	Block other protocols	Operation	
bgpip-000002hl/119.28.217.238	Close	Enable	Enable	Enable	Configuration	
Total items: 1				10 🔻 / page	Image Image <t< td=""><td>ÞI</td></t<>	ÞI

Watermark Protection

Last updated : 2022-03-11 12:30:54

Anti-DDoS supports watermark protection for the messages sent by the application end. Within the range of the UDP and TCP message ports configured, the application end and Anti-DDoS share the same watermark algorithm and key. After the configuration is completed, every message sent from the client will be embedded with the watermark while attack messages will not, so that the attack messages can be identified and discarded. Watermark protection can effectively and comprehensively defend against layer-4 CC attacks, such as analog business packet attacks and replay attacks.

Prerequisites

You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Note:

This feature is a paid service. Please contact us for activation.

Directions

- Log in to the Anti-DDoS console and select Anti-DDoS Advanced (New) > Configurations on the left sidebar.
 Open the DDoS Protection tab.
- 2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxxx".

IP • 200488	Q	IP/Port Protection Domain name protection
		 DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks In Loose Mode, only confirmed attack messages are blocked. In Medium mo blocked. If attack messages failed to be blocked in the Strict mode, or the new Strict Medium Loose

3. Click Set in the Watermark Protection section.

IP Blocklist/Allowlist	Port Filtering
Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.	Block or allow traffic to an Anti-DDoS Advanced IP by specifying the source and destination port range
Configured 4 blocklists, 1 allowlists Set	Configured 1 rules Set
Block by protocol	Watermark Protection
Block requests of the specified protocol according to the traffic to Anti-DDoS. If your application does not use UDP, it's recommended to block all UDP requests.	The application end and Anti-DDoS share the same watermark algorithm and key. In this case, every message sent out from the client is embedded with the watermark, so as to defense layer-4 CC attacks, such as
Configured 1 rules Set	Enabled 1 rules Set

- 4. Click Create.
- 5. In the pop-up window, fill in the configuration fields and click $\ensuremath{\text{OK}}$.

Create a Watermark Protection Policy					
Associate Anti-DDoS Advanced	bgpip-00000488 😆				
Watermark Check Mode	O Normal O Compact				
Port	Protocol Port				
	Add				
Watermark offset					
	OK Cancel				

6. After the rule is created, it is added to the list. You can click **Key Configuration** to view and configure a key.

Watermark Protect	tion				×
Create				Enter IP	Q
Associated Reso	Protocol Port	Offset	Check Mode	Status	Operation
	Т	1	Normal		Delete Key Configuration
Total items: 1			10 👻 / page	e 🛛 🚽 1	/1 page 🕨 🕨

7. You can view and copy the key.

÷	Watermark Protection				
	Create				Enter IP Q
	Associated Resource	Protocol port	Status	Operation	
	bgpip-000002hl/119.28.217.238	TCP-80	Run Now	Delete Key Con	figuration
	Total items: 1			10 🔻 / page	I /1 page ►

8. You can also add or delete a key on the key configuration page. A key can be deleted if you have another key. Up to two watermark keys can be created.

_				
(i) Each application can have up to 2	keys. To add a new key, please delete	e the old key first. When	there is only on valid key, it cann	ot be deleted.
ey		Status	Generation Time	Operation
26a8365c2c203ec-5bba-b26a8365c2c20)3ece093f421bc36e78c12b37e60	Enabled	2020-07-01 22:11:13	Copy Delete
26a8365c2c203ec-5bba-b26a8365c2c20)3ec9acbab02bc36e78ce329a1db	Enabled	2020-07-01 22:11:16	Copy Delete

Feature Filtering

Last updated : 2022-03-11 12:28:20

Anti-DDoS supports configuring custom blocking policies against specific IP, TCP, UDP message header or payload. After enabling feature filtering, you can combine the matching conditions of the source port, destination port, message length, IP message header or payload, and set the protection action to continue protection, allow/block/discard matched requests, block the IP for 15 minutes, or discard the request and then block the IP for 15 minutes, etc. With feature filtering, you can configure accurate protection policies against business message features or attack message features.

Prerequisites

You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Directions

- Log in to the Anti-DDoS console and select Anti-DDoS Advanced (New) > Configurations on the left sidebar.
 Open the DDoS Protection tab.
- 2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxx".

IP • 000488	Q	IP/Port Protection Domain name protection
		 DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks In Loose Mode, only confirmed attack messages are blocked. In Medium mo blocked. If attack messages failed to be blocked in the Strict mode, or the new Strict Medium Loose



3. Click Set in the Port Filtering section to enter the port filtering page.

Block by location Block requests to access Anti-DDoS Advanced instances from IP addresses in specific	ied regions.	IP/Port Speed	Limit Controls access to the business IP by configuring speed limits on IPs and ports.	
Configured 1 rules	Set	Configured	1 rules	Set
Feature Filtering Configure custom blocking policy against specific IP, TCP, UDP message header or policy	ayload.			
Configured 2 rules	Set			

- 4. Click Create.
- 5. In the pop-up window, fill in the configuration fields, and click **OK**.

ssociate Anti-DDoS Advance	bgpip-000002hl 🛞					
Filter feature	Field Logic		Value			
	Source Port 🔻 equals to	•	5000		Delete	
	Destination por 👻 equals to	•	808		Delete	
	Message length equals to	•	1350		Delete	
	IP header 🔻 Find matching	git 💌	ddos	Byte offset Delete	Start	End
	Payload 👻 Find matching	git 🔻	ae86	Byte offset Delete	Start	End
	Add					
Action	Allow O Block Discard) Rejec	t requests and blo	ck IP for 15 m	nins	

6. After the rule is created, it is added to the list. You can click **Configuration** on the right of the rule to modify it.

÷	Feature Filtering					
	Create				Enter IP	Q
	ID	Associated Resource	Feature List	Action	Operation	
	00gipjkv	bgpip-000002hl/119.28.217.238	Source port equals to 5000 Destination port equals to 808 Message length equals to 1350 IP headerFind matching letems via regexddos,Offset byte starts at 5, ends at 60 and PayloadFind matching items via regexae86,Offset byte starts at 5, ends at 60	Allow	Configuration Delete	
	Total items: 1			10	0 🔻 / page 🛛 4 1 / 1 page 🕨 🕨	н

AI Protection

Last updated : 2022-03-11 12:28:20

Anti-DDoS allows you to enable AI protection for powerful defense effect. With AI protection enabled, Anti-DDoS will learn connection baselines and traffic features using algorithms, auto-tune its cleansing policies, and detect and block 4-layer CC attacks.

Prerequisites

You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Directions

- Log in to the Anti-DDoS console and select Anti-DDoS Advanced (New) > Configurations on the left sidebar.
 Open the DDoS Protection tab.
- 2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxx".

IP + Q	IP/Port Protection Domain name protection
	 DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks messages do not compliant with the protocol specifications, and blocks abnormal TCP connections. In Loose Mode, only confirmed attack messages are blocked. In Medium mode, highly-suspicious attack messages are blocked. In Strict mode, all suspicious messages are blocked. In Strict mode, all suspicious messages are blocked if attack messages failed to be blocked in the Strict mode, or the normal messages are blocked in Loose mode, please contact our technical support. Strict O Medium C Loose



3. Click

in the **AI Protection** section to enable the setting.

Connection Attack Protection Set refined protection policies targeting connection attacks	Al Protection The Al engine learns the connection number baseline and traffic characteristics, discovers and blocks layer-4 connection CC attacks, and can effectively defend against layer-4 connection attacks.
Configured 1 rules Set	Defense status
Block by location Block requests to access Anti-DDoS Advanced instances from IP addresses in specified regions.	IP/Port Speed Limit Controls access to the business IP by configuring speed limits on IPs and ports.
Configured 1 rules Set	Configured 1 rules Set

IP Blocklist/Allowlist

Last updated : 2023-04-28 16:48:50

Anti-DDoS supports configuring IP blocklist and allowlist to block or allow source IPs accessing the Anti-DDoS services, restricting the users accessing your business resources. If the accessing traffic exceeds the cleansing threshold, the allowed IPs will be allowed to access resources without being filtered by any protection policy; while the access requests from the blocked IPs will be directly denied.

Prerequisites

You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Note:

The IP blocklist/allowlist will take effect after being created.

- The allowed IPs will be allowed to access resources without being filtered by any protection policy.
- The access requests from the blocked IPs will be directly denied.

Directions

- Log in to the Anti-DDoS console and select Anti-DDoS Advanced (New) > Configurations on the left sidebar.
 Open the DDoS Protection tab.
- 2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxxx".

IP • 000488	2	IP/Port Protection	Domain name protection	
		DDoS Protection Anti-DDoS collects an In Loose Mode, only o blocked. If attack mes Strict Media	Level Id analysis the characteristics of h confirmed attack messages are bl sages failed to be blocked in the um Loose	istory attacks, blocks ocked. In Medium mo Strict mode, or the no

3. Click Set in the "IP blocklist/allowlist" section.

Protection Policy 🛈	
IP Blocklist/Allowlist Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.	Port Filtering Block or allow traffic to an Anti-DDoS Advanced IP by specifying the source and destination port range
Configured 4 blocklists, 1 allowlists	Configured 1 rules Set
Block by protocol	Watermark Protection
Block requests of the specified protocol according to the traffic to Anti-DDoS. If your application does not use UDP, it's recommended to block all UDP requests.	The application end and Anti-DDoS share the same watermark algorithm and key. In this case, every message sent out from the client is embedded with the watermark, so as to defense layer-4 CC attacks, such as
Configured 1 rules Set	• Enabled 1 rules Set

4. Click Create. In the pop-up window, tick Blocklist or Allowlist as the type, enter the target IP, and click OK.

Create IP blacklist/whitelist			
Associate Anti-DDoS Advance	bgpip-000002hl 😒		
Туре	O Blacklist O Whitelist		
IP	1.1.1.1 2.2.2.2	\bigotimes	
	OK Cancel		

5. (Optional) After the rule is created, it is added to the rule list. To delete it, click **Delete** in the "Operation" column on the right.



Associated Resource	Source New Connection Rat	Source Concurrent Connecti	Destination New Connection	Destination Concurrent Con	Maximum Source IP Excepti	Operation
	Close	Close	Close	Close	Close	Configuration

Port Filtering

Last updated : 2022-03-11 12:28:20

Anti-DDoS Advanced enables you to block or allow inbound traffic by ports. With port filtering enabled, you can customize port settings against inbound traffic, including the protocol type, source port and destination port ranges and set the protection action (allow/block/discard) for the matched rule.

Prerequisites

You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Directions

- Log in to the Anti-DDoS console and select Anti-DDoS Advanced (New) > Configurations on the left sidebar.
 Open the DDoS Protection tab.
- 2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxx".

DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, block In Loose Mode, only confirmed attack messages are blocked. In Medium blocked. If attack messages failed to be blocked in the Strict mode, or the Strict O Medium O Loose	IP ▼ Q	IP/Port Protection Domain name protection
		DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks In Loose Mode, only confirmed attack messages are blocked. In Medium m blocked. If attack messages failed to be blocked in the Strict mode, or the r


3. Click Set in the Port Filtering section to enter the port filtering page.

Protection Policy (
IP Blocklist/Allowlist Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.	Port Filtering Block or allow traffic to an Anti-DDoS Advanced IP by specifying the source and destination port range
Configured 4 blocklists, 1 allowlists Set	Configured 1 rules Set
Block by protocol Block requests of the specified protocol according to the traffic to Anti-DDoS. If your application does not use UDP, it's recommended to block all UDP requests.	Watermark Protection The application end and Anti-DDoS share the same watermark algorithm and key. In this case, every message sent out from the client is embedded with the watermark, so as to defense layer-4 CC attacks, such as
Configured 1 rules Set	• Enabled 1 rules Set

4. Click Create, enter the required fields based on the action you select, and then click Save.

Note :
 Multiple instances can be created at a time. For instances without protected resources, you cannot create rules.
• For Priority , enter an integer between 1-1000. A rule with a lower number has higher priority and is listed higher. Default: 10.

Port Filtering							×
Create						Enter IP	Q
Associated Resource	Protocol	Source Port Range	Destination Port Range	Action	Priority (Operation	
bg,	Il Protocols 🔻	-		Discard 💌		Save	Cancel
Total items: 0					10 🔻 / page		/1 page 🕨 🕨

6. After the rule is created, it is added to the rule list. You can click **Configuration** on the right of the rule to modify it.

Associated Resource	Protocol	Port	Speed Limited Mode	Packet rate limit	Operation
bgp	SMP;UDP	-	By source IP		Configuration Delete

Regional Blocking

Last updated : 2022-03-11 12:28:20

This feature allows you to block traffic from source IP addresses in specific geographic locations at the cleansing node, with just one click. You can block traffic from whatever regions or countries you need.

Note :

After you configure the regional blocking setting, attack traffic targeting the region will still be recorded but will not be allowed to your real server.

Prerequisites

You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Directions

- Log in to the Anti-DDoS console and select Anti-DDoS Advanced (New) > Configurations on the left sidebar.
 Open the DDoS Protection tab.
- 2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxxx".





3. Click Set in the Block by Location section for configuration.

Block by location Block requests to access Anti-DDoS Advanced instances from IP addresses in specified regions.	IP/Port Speed Limit Controls access to the business IP by configuring speed limits on IPs and ports.
Configured 1 rules Set	Configured 1 rules Set
Feature Filtering Configure custom blocking policy against specific IP, TCP, UDP message header or payload.	
Configured 2 rules Set	

- 4. Click Create.
- 5. In the pop-up window, select a region to block and click **OK**.

Create Regional Bloc	cking Policy	×
Associate Service Packs	Search by IP or name	
Blocked Areas	China Outside China Custom	
	Confirm	

6. Now the new rule is added to the list. You can click **Configuration** on the right of the rule to modify it.

Associated Resource	Blocked Areas	Operation
bg	-	Configuration Delete

IP and Port Rate Limiting

Last updated : 2022-03-11 12:28:20

Anti-DDoS Advanced allows you to limit traffic rate for application IPs and ports.

Prerequisites

You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Directions

- Log in to the Anti-DDoS console and select Anti-DDoS Advanced (New) > Configurations on the left sidebar.
 Open the DDoS Protection tab.
- 2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxx".

IP • Q	IP/Port Protection Domain name protection
	 DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks In Loose Mode, only confirmed attack messages are blocked. In Medium mo blocked. If attack messages failed to be blocked in the Strict mode, or the new Strict Medium Loose

3. Click Set in the IP/Port Speed Limit section.

Block by locat	ion Block requests to access Anti-DDoS Advanced instances from IP addresses ir specified regions.	1	IP/Port Speed Lin	mit Controls access to the business IP by configuring speed limits on IPs and po	rts.
Configured	1 rules	Set	Configured 1 n	ules	Set
Feature Filteri	ng Configure custom blocking policy against specific IP, TCP, UDP message hear payload.	der or			
• Configured	2 rules	Set			

- 4. Click Create.
- 5. In the pop-up window, select a protocol for the port you set, set a rate limit, and then click **OK**.

Create IP/Port Speed	l Limit	×
Associate Service Packs		
Protocol	ALL TCP UDP SMP Custom	
Port	Please enter port numbers or port ranges; one entry per line; up to 8 entries can be entered. Port range: 0-65535	
Speed Limited Mode	By source IP 💌	
Speed Limit 🕥	bps pps	
	Confirm	



6. After the rule is created, it is added to the list. You can click **Configuration** on the right of the rule to modify it.

Associated Resource	Protocol	Port	Speed Limited Mode	Packet rate limit	Operation
bgr	SMP;UDP	-	By source IP		Configuration Delete

Connection Attack Protection

Last updated : 2022-06-10 14:12:06

Anti-DDoS Advanced can automatically trigger blocking policies facing abnormal connections. With **Maximum Source IP Exceptional Connections** enabled, a source IP that frequently sends a large number of messages about abnormal connection status will be detected and added to the blocklist. The source IP will be accessible after being blocked for 15 minutes. You can set the following configurations as needed:

Note:

- Source New Connection Rate Limit: It limits the rate of new connections from source ports.
- Source Concurrent Connection Limit: It limits the number of active TCP connections from source addresses at any one time.
- Destination New Connection Rate Limit: It limits the rate of new connections from destination IP addresses and destination ports.
- **Destination Concurrent Connection Limit**: It limits the number of active TCP connections from destination IP addresses at any one time.
- Maximum Source IP Exceptional Connections: It limits the maximum number of abnormal connections from source IP addresses.

Prerequisites

You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Directions

Log in to the Anti-DDoS console and select Anti-DDoS Advanced (New) > Configurations on the left sidebar.
 Open the DDoS Protection tab.

2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxxx".

IP • Q	IP/Port Protection Domain name protection
	 DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks In Loose Mode, only confirmed attack messages are blocked. In Medium m blocked. If attack messages failed to be blocked in the Strict mode, or the r Strict Medium Loose

3. Click Set in the Connection Attack Protection to enter the configuration page.

Protection Policy (j)	
IP Blocklist/Allowlist Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource. Set	Al Protection The Al engine learns the connection number baseline and traffic characteristics, discovers and blocks layer-4 connection CC attacks, and can effectively defend against layer-4 connection attacks. Set
Connection Attack Protection	ID/Dat Speed Limit
Set refined protection policies targeting connection attacks	Controls access to the business IP by configuring speed limits on IPs and ports.
Set	Set

4. Click **Create** to create a connection attack protection rule.



5. In the pop-up window, enable Abnormal Connection Protection, and click OK.



6. After the rule is created, it is added to the list. You can click **Configuration** on the right of the rule to modify it.

Associated Resource	Source New Connection Rat	Source Concurrent Connecti	Destination New Connection	Destination Concurrent Con	Maximum Source IP Excepti	Operation
1	Close	Close	Close	Close	Close	Configuration

CC protection Protection Level and Cleansing Threshold

Last updated : 2022-03-02 13:25:43

Protection Description

"CC Protection" identifies and blocks CC attacks based on access attributes and connection status. It provides scenario-specific configurations to create protection rules, helping secure your business. It also supports the cleaning threshold setting.

Prerequisites

You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Directions

- Log in to the Anti-DDoS console and select Anti-DDoS Advanced (New) > Configurations on the left sidebar.
 Open the CC Protection tab.
- 2. Select a domain name from the IP list.



3. To enable CC protection in the "CC Protection and Cleansing Threshold" section, click and set a cleansing threshold.

Configurations DDoS Protection CC Protection	B Global Setting Mode
Protection Flow Non-website/port user Vesster/domain User User Division User Division Vesster/domain name applications DOS Engine Real Service DOS Engine Real Service Real Ser	Different protection policies are applicable to different engines: Troubleshooting IP/port protection policy is applicable to the Anti-DDoS engine, and er the domain name protection policy is applicable to the CC Why are there illimits on the manual unblocking times? And what are the limits? View Alt View Alt er the domain name protection engine, and protection engine. Why are there illimits on the manual unblocking times? And what are the limits? View Alt
IP Y Q	For details about configuring domain name protection, contact your sales rep
bgo bgo	C Protection and Cleansing Threshold () CC protection detects malicious behaviors according to access modes and connection status. In Losse Mode, only confirmed attack requests are blocked. In Medium mode, highly-suspicious requests are blocked. In Strict mode, all suspicious requests are blocked
bgp bgp	Cleansing Threshold () 1-20000 QPS Set

Note :

- This switch controls wether to enable CC protection. Only when it is on, all the CC protection policies take effect.
- The cleansing threshold is the threshold for Anti-DDoS services to start cleansing traffic. If the number of HTTP requests sent to the specified domain name exceeds the threshold, CC protection will be triggered.
- If the protection is enabled, your Anti-DDoS Advanced instance will use the default cleansing threshold after your business is connected, and the system will generate a baseline based on historical patterns of your business traffic. You can also set the cleansing threshold for your business needs.
- If you have a clear concept about the threshold, set it as required. Otherwise please leave it to the default value. Anti-DDoS will automatically learn through AI algorithms and generate the default threshold for you.

Intelligent CC Protection

Last updated : 2023-04-28 16:48:50

Intelligent CC protection is an AI-powered protection feature leveraging Tencent Cloud's big data capability. It provides a dynamic protection model to auto-generate rules for detecting and blocking malicious attacks based on website traffic patterns and algorithm-utilized attack analysis.

Prerequisites

- You have purchased an Anti-DDoS Advanced instance and set the object to protect.
- Only rules configured for instances accessing via domain names take effect.

Directions

- Log in to the Anti-DDoS console. Select Anti-DDoS Advanced (New) > Configurations on the left sidebar. Open the CC Protection tab.
- 2. Select a domain name from the IP list on the left.

3. In the "CC Protection and Cleansing Threshold" card, click

IP v Q	For details about configuring domain name protection, contact your sales rep	^
bg 🗧 🗧 o	E CC Protection and Cleansing Threshold (
pât	CC protection detects malicious behaviors according to access modes and connection status. In Loose Mode, only confirmed attack requests are blocked. In Medium mode, highly- suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. If attack requests failed to be blocked in the Strict mode, or the normal requests are blocked in Loose mode, please contact our technical support.	
bgr	CC Protection O When it's off, the following CC protection policies do not take effect	
bgp-		Set



and set a cleansing threshold before enabling

Note :

intelligent CC protection.

- The cleansing threshold is the threshold for Anti-DDoS services to start cleansing traffic. If the number of HTTP requests sent to the specified domain name exceeds the threshold, CC protection will be triggered.
- If the IP bound to the Anti-DDoS Pro instance is from WAF, you need to first enable CC protection for the IP in the WAF console. For more information, see CC Protection Rules.



E CC Protection and Cleansing Threshold 🕄	
CC protection detects malicious behaviors according to access modes and connection status. In Loose Mode, only confirmed attack requests are blocked. In Medium mod suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. If attack requests failed to be blocked in the Strict mode, or the normal requests are blocked Loose mode, please contact our technical support.	e, highly- ocked in
CC Protection When it's off, the following CC protection policies do not take effect	
Cleansing Threshold (1~20000 QPS	Set
4. In the Intelligent CC protection card, toggle on the switch.	
CC Protection and Cleansing Threshold (i) CC protection detects malicious behaviors according to access modes and connection status. In Loose Mode, only confirmed attack requests are blocked. In Medium mode suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. If attack requests failed to be blocked in the Strict mode, or the normal requests are blo loose mode plocked on the Strict mode, all suspicious requests are blocked. If attack requests failed to be blocked in the Strict mode, or the normal requests are blocked.	, highly- cked in
CC Protection When it's off, the following CC protection policies do not take effect	
Cleansing Threshold ① 1~20000 QPS	Set
CC AI Protection After enabling CC AI protection, based on Tencent Cloud's big data capabilities, CC AI protection can self-learn website business traffic baselines, analyze attack anomalies combination with algorithms, automatically issue accurate protection rules, and dynamically adjust business protection models to help you discover and prevent timely Block attacks.	in malicious Set

5. Click **View** to view the auto-generated protection rules. You can make changes to these rules if necessary.

Note :

- When intelligent CC protection is enabled, the protection rules are auto-generated when an attack occurs.
- Protect mode: Apply auto-generated protection rules to defend against each specific attack. After the attack ends, the rules are automatically deleted.
- Observe mode: Attacks are observed only.



CC AI Protection

After enabling CC AI protection, based on Tencent Cloud's big data capabilities, CC AI protection can self-learn website business traffic baselines, analyze attack anomalies in combination with algorithms, automatically issue accurate protection rules, and dynamically adjust business protection models to help you discover and prevent timely Block malicious
attacks. Set
After CC AI Protection is enabled, CC AI Protection automatically generates protection rules based on each attack. The rules issued by intelligent protection have a single validity period. After a single attack ends, the protection rules are automatically invalidated and cleared. Adjust if necessary for the next attack. Please click View on the right to edit smart protection rules.

6. To delete a rule, click **Delete** on the right of the rule you want to remove.

C AI Protection Enable			×
ne following CC AI protection otection have a single validit otection rules can be deleted	rules are automatically generat y period. After a single attack er d based on protection requireme	ed and take effect based on a single attack. The notection rules are automatically invations.	he rules issued by intelligent lidated and cleared. The following
IP v	Q		
Match Condition	policy	effective time	Operation
		No data yet	
		10 🔻 / page	1 / 1 page >>

Precise Protection

Last updated : 2022-12-21 17:50:10

Use Cases

Anti-DDoS supports precise protection for connected web applications. With the precise protection, you can configure protection policies combining multiple conditions of common HTTP fields, such as URI, UA, Cookie, Referer, and Accept to screen access requests. For the requests matched the conditions, you can configure CAPTCHA to verify the requesters or a policy to automatically drop or allow the requests. Precise protection is available for policy customization in various use cases to precisely defend against CC attacks.

The match conditions define the request characteristics to be checked, i.e., the attribute characteristics of the HTTP field in a request. Precise protection supports checking the HTTP fields below:

Match Field	Field Description	Logic
URI	The URI of an access request.	Equals to, includes, or does not include.
UA	The identifier and other information of the client browser that initiates an access request.	Equals to, includes, or does not include.
Cookie	The cookie information in an access request.	Equals to, includes, or does not include.
Referer	The source website of an access request, from which the access request is redirected.	Equals to, includes, or does not include.
Accept	The data type to be received by the client that initiates the access request.	Equals to, includes, or does not include.

Prerequisites

You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Directions



1. Log in to the Anti-DDoS console and select Anti-DDoS Advanced (New) > Configurations on the left sidebar.

Open the CC Protection tab.

2. Select a domain name from the IP list on the left.

DDoS Protection CC Protection			
Protection Flow User User Vebsite/domain name applications DDoS Engine Cc Engine	Different IP/port p Real Server the dom protectio	ant protection policies are applicable to different engines: Troubleshooting Why are there limits on the manual unbiodding times? And what are the limits? t protection policy is applicable to the Anti-DDoS engine, and anname protection policy is applicable to the CC other engine.	View A
lb a	۲ For details	ils about configuring domain name protection, contact your sales rep	
* 4	с со	CC Protection and Cleansing Threshold ()	
K	CC pro are blo	vrotection detects malicious behaviors according to access modes and connection status. In Loose Mode, only confirmed attack requests are biocked. In Medium mode, highly-suspicious requests are biocked. In Strict mode, all suspicious requests failed to be biocked in the Strict mode, or the normal requests are biocked in Loose mode, please contact our technical support.	uests
h	CC Pro Cleans	rotection When it's off, the following CC protection policies do not take effect insing Threshold Custom QPS	

3. Click Set in the Precise Protection section to enter the rule list.

Block by location Block requests to access Anti-DDoS Advanced instances from IP addresses in specific	regions.	Allowlist Configure IP blocklist and allowlist to block or allow requests from sp define who can access your application resource.	pecific source IPs, so as to
Configured 1 rules	Set • Configured	5 rules (max: 50 rules)	Set
Precise Protection A protection policy with a combination of conditions of common HTTP fields	CC Frequenc	y Limit Set a limit to control to access frequency from the source IP.	
Configured 1 rules	Set Defense Status	Defense Level ① Urgent 💌	Set



4. Click **Create** to create a precise protection rule. Fill in the fields and click **OK**.

Create Precise Protection	Policy	×
Associate Anti-DDoS Advance	bgpip-000002j1 😢	
IP	153.3.137.126	
Protocol		
Domain name	test.probe.tencentdayu.com 🔻	
Condition	Field Logic Value	
	uri 💌 equa 💌 / Delete	
	ua ▼ equa ▼ chrom∈ Delete	
	cook 💌 equa 💌 4d5a Delete	
	refer v equa v Delete	
	Add	
Match Operation	Discard	
	OK Cancel	



5. Now the new rule is added to the rule list. You can click **Configuration** on the right of the rule to modify it.

÷	Precise Protection							
	Create							
	ID	Associated Resource	Protocol	Domain name	Condition	Match Operation	Creation Time	Operation
	ccPrecs-00000ouy	bgpip- 000002j1/153.3.137.126	http	test.probe.tencentdayu.co m	uri equals to / cookie equals to 4d5a ua equals to chrome	Discard	2020-07-06 14:59:38	Configuration Delete
	ccPrecs-00000out	bgpip- 000002j1/153.3.137.126	http	test.probe.tencentdayu.co m	uri equals to /	CAPTCH	2020-06-30 20:32:07	Configuration Delete
	Total items: 2						10 🔻 / page 📕 🖣	1 / 1 page 🕨 🕨

CC Frequency Limit

Last updated : 2020-07-07 17:19:14

Prerequisites

You need to purchase an Anti-DDoS Advanced instance and set the protected object first.

Directions

- 1. Log in to the new Anti-DDoS Advanced Console and select Protection Configuration on the left sidebar.
- Select a domain name under the ID of an Anti-DDoS Advanced instance in the list on the left; for example, select "212.64.xx.xx bgpip-000002je" > "http:80" > "www.xxx.com".

÷	IP Black/White List					
	Create				Enter IP	Q
	Associated Resource	Туре	ip	Operation		
		Nc	o data yet			
	Total items: 3			10 🔻 / page	H 4 1 /1 page >	M

3. Click Set in the "CC Frequency Limit" block on the right to enter the frequency limit rule list.

CC Freq	CC Frequency Limit											
Create												
ID	Bound Resource	Protocol	Domain name	Detection Perio	Detection Times	Match Type	Match value	Action	Creation Time	Operation		
					No data yet							
Total items	: 0							10 🔻 / page		/1 page 🕨 🕅		



4. Click Create to create a frequency limit rule, fill in relevant fields, and click OK.

Create CC Frequency Lim	it	×
Associate Anti-DDoS Advance	bgpip-0000015s 😒	
IP	150.109.141.216	
Protocol		
Domain name	Please select	
	Field Mode Value	
	Uri 💌 equa 💌 / Delete	
	Add	
Frequency Limit Policy	САРТСН	
Condition	When 10 secol • Access 100 Times	
Punishment Time	3600 seconds 🔗	
	OK Cancel	

5. After the creation is completed, a frequency limit rule will be added to the frequency limit list. You can modify the rule by clicking **Configure** in the "Operation" column on the right.

c	C Frequency I	Limit									
	Create										
	ID	Bound Resource	Protocol	Domain name	Detection Perio	Detection Times	Match Type	Match value	Action	Creation Time	Operation
	ccRule-000000cg	bgpip- 00000209/212.64. 62.249	http	prob1.probe.tence ntdayu.com	10	1	Uri	/	CAPTCH	2020-06-02 11:24:24	Configuration Delete
	Total items: 1								10 🔻 / page		/1 page 🕨 🕨

Regional Blocking

Last updated : 2022-03-11 12:28:20

Anti-DDoS Advanced allows you to block website access requests from source IP addresses in specific geographic locations, with just one click. You can block all website access requests from whatever regions or countries you need.

Note :

After you configure the regional blocking setting, attack traffic targeting the region will still be recorded but will not be allowed to your real server.

Prerequisites

You have purchased an Anti-DDoS Advanced instance, set your target to protect, and connected to domain names.

Directions

- Log in to the Anti-DDoS console and select Anti-DDoS Advanced (New) > Configurations on the left sidebar.
 Open the CC Protection tab.
- 2. Select a domain name from the IP list on the left.





3. Click Set in the Block by Location section for configuration.

Block by location Block requests to access Anti-DDoS Advanced instances from IP addresses in specified regions.	IP Blocklist/Allowlist Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.
Configured 1 rules Set	Configured 5 rules (max: 50 rules) Set
Precise Protection A protection policy with a combination of conditions of common HTTP fields	CC Frequency Limit Set a limit to control to access frequency from the source IP.
Configured 1 rules Set	Defense Status 🚺 Defense Level 🛈 Urgent 💌

4. Click Create.

Create			Enter IP	Q
Associated Resource	Blocked Areas	Operation		
	No data yet			

5. In the pop-up dialog, select an IP, a protocol, domain name, and region. Click OK.

Create Regi	onal Blocking Policy			×
Associate Serv	ice Packs bgp-000001cg			
IP	Please select	▼		
Protocol	• НТТР			
Domain				
Blocked Areas	O China Outside	China Custom	_	
		Confirm	Cancel	

6. Now the new rule is added to the list. You can click **Configuration** on the right of the rule to modify it.

Associated Resource	Protocol	Domain	Blocked Areas	Operation
bgp-0000 218		5/	China	Configuration Delete

IP Blocklist/Allowlist

Last updated : 2022-03-02 13:25:43

Anti-DDoS Advanced supports IP blocklist and allowlist configurations to block and allow IPs connected to Anti-DDoS Advanced, restricting the users from accessing your resources. For the allowed IPs, they are allowed to access without being filtered by any protection policy; while the access requests from the blocked IPs are directly denied.

Note :

The IP blocklist and allowlist filtering takes effect only when your business is under CC attacks.

- The allowed IPs will be allowed to access resources without being filtered by any protection policy.
- The access requests from the blocked IPs will be directly denied.

Prerequisites

You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Directions

- 1. Log in to the Anti-DDoS console and select Anti-DDoS Advanced (New) > Configurations on the left sidebar. Open the CC Protection tab.
- 2. Select a domain name from the IP list on the left.

DDoS Protection CC Protection Protection Flow Non-website/port application User Website/domain name applications DDoS Engine	CC Engine Real Server	Troubleshooting Different protection policies are applicable to different engines: Why are three limits on the manual unblocking times? And what are the limits? IP/port protection policy is applicable to the Anti-DDoS engine, and the domain name protection policy is applicable to the CC How can I connect to a blocked server? Attack-related FAQ Attack-related FAQ	View All
р ч ч	Q	Per details about configuring domain name protection, contact your sales rep C C Protection and Cleansing Threshold () CC protection detects malicious behaviors accounding to access modes and connection status. In Loose Mode, only confirmed attack requests are blocked. In Medium mode, highly-suspicious requests are blocked. In Strict mode, all suspicious re blocked. If attack requests failed to be blocked in the Strict mode, all suspicious re blocked. If attack requests failed to be blocked in the Strict mode, all suspicious re blocked. If attack requests failed to be blocked in the Strict mode, all suspicious re blocked. If attack requests failed to be blocked in the Strict mode, all suspicious re blocked. If attack requests failed to be blocked in the Strict mode, only confirmed attack requests are blocked. In Strict mode, all suspicious re blocked. If attack requests failed to be blocked in the Strict mode, only confirmed attack requests are blocked. In Strict mode, all suspicious re blocked. If attack requests failed to be blocked in the Strict mode, only confirmed attack requests are blocked. In Strict mode, all suspicious re blocked. If attack requests failed to be blocked in the Strict mode, only confirmed attack requests are blocked. In Strict mode, all suspicious re blocked. If attack requests failed to be blocked in the Strict mode, all suspicious re blocked. If attack requests failed to be blocked. In Strict mode, all suspicious re blocked. If attack requests failed to be blocked in the Strict mode, all suspicious re blocked. If attack requests failed to be blocked. In Strict mode, all suspicious re blocked. If attack requests failed to be blocked. In Strict mode, all suspicious re blocked. If attack requests failed to be blocked. In Strict mode, all suspicious re blocked. If attack requests failed to be blocked. In Strict mode, all suspicious re blocked. If attack requests failed to be blocked. If attack requests failed to be blocked. If attack requests failed to be blocked. If attack requests fa	iquests



3. Click Set on the IP Blocklist/Allowlist section.

For details about configuring domain name protection, contact your sales rep	
CC Protection and Cleansing Threshold ① CC protection detects malicious behaviors according to access modes and connection status. In Loose Mode, only confirmed are blocked. If attack requests failed to be blocked in the Strict mode, or the normal requests are blocked in Loose mode, ple	i attack requests are blocked. In Medium mode, highly-suspicious requests are blocked. In Strict mode, all suspicious requests ase contact our technical support.
CC Protection When it's off, the following CC protection policies do not take effect Cleansing Threshold () 2 QPS	Set
Block by location Block requests to access Anti-DDoS Advanced instances from IP addresses in specified regions.	IP Blocklist/Allowlist Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.
Configured 1 rules Set	Configured 1 rules (max: 50 rules)

4. Click Create, and enter the required fields before you click Save.

IP Blocklist/Allowlist							×
Create						Enter an IP	Q
Associated Resource	Associated IP	Protocol Type	Domain Name	Blocked/Allowed IPs	Туре Т	Modification Time	Operation
bgp-û		http 🔻			Blocklist 👻		Save Cancel
bgp-f		http		1	Blocklist	2021-12-27 22:10:23	Set Delete
Total items: 1					10 💌 / page		/1 page 🕨 🕷

5. Now the rule is added to the list. You can click **Delete** on the right of the rule to delete it.

IP Blocklist/Allowlist								×
Create						Enter an IP		Q
Associated Resource	Associated IP	Protocol Type	Domain Name	Blocked/Allowed IPs	Туре Т	Modification Time	Operation	
bg.		http	a		Blocklist	2021-12-27 22:10:23	Set Delete	
Total items: 1					10 🔻 / page		/1 page →	

Business Connection Port Connection

Last updated : 2023-04-28 16:48:50

Note :

Note that the DNS address should be changed to the CNAME address provided, which will be updated (Non-BGP resources are not supported).

Accessing a Rule

- 1. Log in to the Anti-DDoS Advanced Console, select Anti-DDoS Advanced (New) > Application Accessing on the left sidebar, and then open the Access via ports tab.
- 2. Click Start Access.

cation Ac	cessing								P
ess via por	ts Ac	cess via domain na	mes						
Forwa	Forwa	Origin Server P	Origin	Associated Protectin	Load Balancing Mode	Health check	Session Persistence	Modification Time	Operation
TCP	41900	80	150.158.199.231	212.64.62.249	Weighted polling	Close Edit	Close Edit	2020-07-02 11:22:35	Configuration Delete
TCP	234	234	119.29.205.248	150.109.130.57	Weighted polling	Not supported	Not supported	2020-06-30 19:27:00	Configuration Delete
TCP	8080	80	134.175.195.228 1.1.1.2	150.109.132.100	Weighted polling	Not supported	Not supported	2020-06-29 16:32:02	Configuration Delete
TCP	80	80	106.52.156.188	117.184.254.214	Weighted polling	Close Edit	Close Edit	2020-06-28 14:45:59	Configuration Delete
TCP	41900	80	49.232.127.41	188.131.208.243	Weighted polling	Close Edit (1)	Close Edit	2020-06-28 10:45:20	Configuration Delete
TCP	41800	80	49.232.127.41	188.131.208.243	Weighted polling	Close Edit (j)	Close Edit	2020-06-28 10:45:17	Configuration Delete
TCP	41700	80	49.232.127.41	188.131.208.243	Weighted polling	Close Edit (1)	Close Edit	2020-06-28 10:45:14	Configuration Delete
TCP	41600	80	49.232.127.41	188.131.208.243	Weighted polling	Close Edit (i)	Close Edit	2020-06-28 10:45:10	Configuration Delete
TCP	31500	80	49.232.127.41	188.131.208.243	Weighted polling	Close Edit (1)	Close Edit	2020-06-28 10:45:07	Configuration Delete
TCP	31400	80	49.232.127.41	188.131.208.243	Weighted polling	Close Edit (j)	Close Edit	2020-06-28 10:45:03	Configuration Delete
Total items	: 159							10 v / page H 4 1	/ 16 pages 🕨 🕨

3. On the Access via Port page, select an associated instance ID and click Next: Set Port Parameter.



Note :

You can select multiple instances.

- 4. Select a forwarding protocol, specify a forwarding port and real server port, and then click **Next: Set Forwarding Method**.
- 5. Select a forwarding method, specify a "real server IP+port"/real sever domain name, and add an alternate real server and set the weight if you have one. Then click **Next: Modify DNS Resolution**.

Note:

- An alternate real server is used when the real server's forwarding fails.
- If the forwarding port you specify in the second step "Set Port Parameter" is occupied, you cannot proceed to the next step.
- 6. Click Complete.

Querying a Rule

On the Access via ports page, enter a real server IP/domain name, real server port, forwarding protocol/port or an associated instance ID in the search box.

Separate multiple keyword	ds with " "							(i) Q
Select a filter Origin IP/Domain Name	Real Server Port	Origin	Associated Protectin	Load Balancing Mode	Health Check	Session Persistence	Modification Time	Operation
Real Server Port		1 9	42 131	Weighted	Disable Edit 🛈	Disable Edit	2021-11-25 21:08:09	Configuration Delete
Associated Protecting IP Forwarding Protocol	-	1 59	56.131	Weighted Round Robin	Disable Edit 🕄	Disable Edit	2021-11-24 20:34:56	Configuration Delete
Forwarding Port		٤ 53	42. 31	Weighted Round Robin	Disable Edit 🛈	Disable Edit	2021-11-24 18:00:03	Configuration Delete

Editing a Rule

- 1. On the Access via ports page, select a rule you want to edit and click **Configuration**.
- 2. On the **Configure Layer-4 Forwarding Rule** page, modify parameters and click **OK** to save changes.

Deleting Rules

- 1. On the Access via ports page, you can delete one or more rules.
 - To delete a rule, select a rule you want to delete. Click **Delete**.
 - To delete multiple rules, select more than one rules you want to delete. Click **Batch Delete**.
- 2. In the pop-up window, click **Delete**.

Importing a Rule

- 1. To import multiple rules, you can click **Batch Import** on the Access via ports page.
- 2. In the **Configure Layer-4 Forwarding Rule** window, enter the rules, and click **OK**.

Exporting a Rule

- 1. To import multiple rules, you can click **Batch Export** on the Access via ports page.
- 2. In the **Batch Export Layer-4 Forwarding Rules** window, select the rules you want to export, and click **Copy**.

Domain Name Connection

Last updated : 2023-04-28 16:48:50

Note:

Note that the DNS address should be changed to the CNAME address provided, which will be updated (Non-BGP resources are not supported).

Accessing a Rule

- 1. Log in to the Anti-DDoS Advanced Console, select Anti-DDoS Advanced (New) > Application Accessing on the left sidebar, and then open the Access via domain names tab.
- 2. Click Start Access.



3. On the Access via Domain Name page, select an associated instance ID and click Next: Set Port Parameter.





Access via Domain N	ame					×
Select Instance Modify DNS Res	> 2 Protocol Po	rt > (3 Set Forward	ding Method	>	
Do	CNAME address/A record	0	Forwarding Port Forwarding	Real Server Port Protocol		
User		Edge Defender	Anti-DDoS	Origin	Real Server	
* Associated Instance	Search by IP or name		Auvanceu	ΙΓ		

3. Select a forwarding protocol, specify a domain name, and then click **Next: Set Forwarding Method**.

Access via Domain Name	×
 Select Instance > 2 Protocol Port > 3 Set Forwarding Method > Modify DNS Resolution 	
CNAME address/A record User CNAME address/A record CNAME address/A record User CNAME address/A record Edge Defender Edge Defender Advanced IP	
 ★ Forwarding Protocol ▶ https 	
* Application domain name	

4. Select a forwarding method, specify a "real server IP+port"/real sever domain name, and add an alternate real



server and set the weight if you have one. Then click **Next: Modify DNS Resolution**.

Access via Domain Na	me	3
 Select Instance Modify DNS Res 	> Protocol Port > 3 Set Forwarding Method > plution	
O User	CNAME address/A record CNAME address/A record Edge Defender Forwarding Port Port Port Port Port Port Port Port	
 * Set Forwarding Method * Beal Server IP & Port 	• Forwarding via IP • Forwarding via domain name Clean traffic can be forwarded back to the real server by the IP or domain name	
	Origin IP Real Server Port Enter the real server (eg: 1.1.1) Eg: 80 Delete	_
	+ Add Please enter the combination of real server IP and port. Up to 16 entries are allowed.	

Note :

An alternate real server is used when the real server's forwarding fails.

5. Click **Complete**. Rules that are added will display in the domain name list. You can check whether they access via the domain names successfully.

Note :

- When the access fails due to certification configuration errors, you will get a prompt "Failed to obtain the certificate. Please go to SSL Certificate Management to view details".
- To avoid seconds of interruptions, update the certificate for connected domain names during off-peak periods.



Start Access	Batch Import	Batch Export Bate	ch Delete					Enter a domain	name or an as	Q
Application do	m Forwarding Pro	t Forwarding Port	Real Server IP/Site	Associated Prote	Health Check	Access Status	CC Protection Stat	Modification Time	Operation	
		-	-		Disable Configuration	Success	Disable 🧻 🤅	2022-04-25 19:04:02	Configuration Delete	
	•				Disable Configuration	Success	Disable Configuration	2022-04-25 19:04:09	Configuration Delete	

Editing a Rule

1. On the Access via domain names page, select a rule you want to edit and click **Configuration**.

Start Access Bate	th Import Batch	Batch De	elete					Enter a domain r	name or an as
Application dom	Forwarding Prot	Forwarding Port	Real Server IP/Site	Associated Prote	Health Check	Access Status	CC Protection Stat	Modification Time	Operation
1000					Disable Configuration	Success	Disable 🚺 🔅	2022-04-25 19:04:02	Configuration Delete
m	-				Disable Configuration	Success	Disable Configuration	2022-04-25 19:04:09	Configuration Delete
					Disable Configuration	Success	Disable 🚺 🕄	2022-04-25 18:59:54	Configuration Delete



2. On the **Configure Layer-7 Forwarding Rule** page, modify parameters and click **OK** to save changes.

Configure Layer-7 Forw	varding Rule	×
Associated Protecting IP	Up to 60 rules can be added, 6 added now	
Domain Name	Please enter a domain name containing up to 67 characters.	
Protocol	http O https	
	Forward via HTTP for HTTPS requests	
Certificate Source	Tencent Cloud Hosting Certificate(C) SSL Certificate Management	
Certificate	▼	
Set Forwarding Method	Forwarding via IP Forwarding via domain name	
Real Server Domain Name	Real Server Domain Name Real Server Port	
	Delete	
	+ Add	
	Please enter the real server domain name (CNAME) or the combination of real server domain name (CNAME) and port. It supports up to 16 entries.	

Deleting Rules

1. On the Access via domain names, you can delete one or more rules.

• To delete a rule, select a rule you want to delete. Click **Delete**.

Start Access Bat	tch Import Batc	h Export Batch	Delete					Enter a domain	name or an as Q
Application dom	Forwarding Prot	Forwarding Port	Real Server IP/Site	Associated Prote	Health Check	Access Status	CC Protection Stat	Modification Time	Operation
_ m	-				Disable Configuration (i)	Success	Disable 🚺 🚯	2022-04-25 19:04:02	Configuration Delete
C m		•		• • • •	Disable Configuration	Success	Disable Configuration	2022-04-25 19:04:09	Configuration Delete

• To delete multiple rules, select more than one rules you want to delete. Click **Batch Delete**.

Start Access Bat	tch Import Bato	ch Export Batch	n Delete					Enter a domain	name or an as	Q
 Application dom 	Forwarding Prot	Forwarding Port	Real Server IP/Site	Associated Prote	Health Check	Access Status	CC Protection Stat	Modification Time	Operation	
✓ m	M.,	in .			Disable Configuration	Success	Disable 🚺 🚯	2022-04-25 19:04:02	Configuration Delete	
	•				Disable Configuration	Success	Disable Configuration	2022-04-25 19:04:09	Configuration Delete	

2. In the pop-up window, click **Delete**.

Importing a Rule

1. To import multiple rules, you can click **Batch Import**.



2. In the Configure Layer-7 Forwarding Rule window, enter the rules, and click ** OK.



Exporting a Rule

1. To import multiple rules, you can click **Batch Export**.



2. In the Batch Export Layer-7 Forwarding Rules window, select the rules you want to export, and click Copy.

Search by IP or name		

Configuring Session Persistence

Last updated : 2022-04-28 14:48:00

The non-website business protection service of Anti-DDoS Advanced provides IP-based session persistence to support forwarding requests from the same IP address to the same real server for processing. Layer-4 forwarding supports simple session persistence. The session persistence duration can be set to any integer between 30 and 3,600 seconds. If the time threshold is exceeded and the session has no new request, the connection will be automatically closed.

Directions

- 1. Log in to the new Anti-DDoS Advanced Console and click Business Connection > Port Connection .
- 2. On the "Port Connection" tab, select the target Anti-DDoS Advanced instance and the corresponding rule and click **Edit** in the "Session Persistence" column.

plication Acc	essing								Pure
ccess via ports	s Ac	cess via domain na	imes						
Add rule	Enter	IP	Q						
Forwa	Forwa	Origin Server P	Origin	Associated Protectin	Load Balancing Mode	Health check	Session Persistence	Modification Time	Operation
TCP	41900	80	150.158.199.231	212.64.62.249	Weighted polling	Close Edit	Close Edit	2020-07-02 11:22:35	Configuration Delete
TCP	234	234	119.29.205.248	150.109.130.57	Weighted polling	Not supported	Not supported	2020-06-30 19:27:00	Configuration Delete

3. On the session persistence editing page, set the persistence duration and click OK.

Note :

Session persistence is disabled by default. When setting the persistence duration, you are recommended to use the default value.




Instance Management Viewing Instance Information

Last updated : 2022-08-16 15:28:12

You can view the basic information (such as the base protection bandwidth and running status) and elastic protection configuration of your purchased Anti-DDoS Advanced instances in the console.

Directions

The following takes the Anti-DDoS Advanced instance "bgpip-000002jf" as an example.

 Log in to the Anti-DDoS Advanced Console. Select Anti-DDoS Advanced (New) > Instance List on the left sidebar. Select a target instance and click the ID to view the instance details. If you have many instances, you can use the search box in the top right corner to filter results.

Instance List									Purchase
S All Regions 🔻	S All Lines 🔻							Enter ID/	'name/IP Q
ID/Name/Tag	IP Protocol	Anti-DDoS Advanced	Specifications	Specifications	Status T	Attacks in last 7 days	Date		Operation
d Not named ∳ None ∳	IPv4		Line: CMCC(Shanghai) Application Bandwidth: 100Mbps Elastic Application Bandwidth: Package type: Non-BGP pack	Base bandwidth peak: 60Gbps Elastic Protection: not enabled e ⁹ CC Protec 1000 000 000	Protection Status Protected ports: 0 Protected domains: 0	0 times 🗠	Purchase time: 04-15	2022-	Configurations View Report

2. On the pop-up page, you can view the following information:

bgpip-000002tb			
Basic Information			
Anti-DDoS Advanced Name	Unnamed 🎤	Current Status	Running
Location	Hong Kong, China	Expiry Time	2020-08-06
IP	119.28.217.248		
Base Protection Bandwidth	50Gbps	Forwarding IP Range	119.28.191.0/24 119.28.44.0/24
CC Protection Peak	150000QPS		119.28.85.0/24
Line	BGP		119.28.3.0/24 119.28.187.0/24
Max forwarding rules	60		119.28.186.0/24 119.28.193.0/24
			119.28.217.0/24

- Anti-DDoS Advanced Name: Name of the Anti-DDos Advanced instance, which allows you to identify and manage instances. You can create a instance name containing 1–20 characters of any type as desired.
- Destination IP: The IP address of Anti-DDoS Advanced instance. The IP address may change.

Note :

To avoid DNS resolution failure, you are recommended to change the DNS resolution address to the assigned CNAME.

- **Region**: Select a region when purchasing an Anti-DDoS Advanced instance.
- **CNAME**: CNAME of the Anti-DDoS Advanced instance. The CNAME will be resolved to an instance IP that can forward cleansed traffic to the origin server.

Note :

To avoid DNS resolution failure, you are recommended to change the DNS resolution address to the assigned CNAME.

- Base protection bandwidth: Base protection bandwidth of the Anti-DDoS Advanced instance, that is, the base protection bandwidth you select when you purchase the instance. If the elastic protection is disabled, the base protection bandwidth is the maximum bandwidth of the instance.
- Current Status: Current status of the Anti-DDoS Advanced instance, such as Running, Cleansing, and Blocking.
- Expiration Time: It is calculated based on the purchase duration selected when the instance is purchased and the time when the order is paid, which is accurate to second. Tencent Cloud will send expiration and renewal reminders to the account creator and all collaborators through Message Center, SMS, and email within 7 days before the instance expires.
 - Tag: Tag of the Anti-DDoS Advanced instance, which can be edited and deleted.
 - Intermediate IP Range: IP that forwards cleansed traffic back to the origin server.

Setting Instance Alias and Tag

Last updated : 2020-07-07 17:19:16

When multiple Anti-DDoS Advanced instances are used, you can set "resource names" to quickly identify and manage them.

Prerequisites

You need to purchase an Anti-DDoS Advanced instance first.

Directions

Method 1

- 1. Log in to the new Anti-DDoS Advanced Console and click Instance List on the left sidebar.
- 2. In the instance list, click the second row in the "ID/Name/Tag" column of the target instance and enter a name.

The name can contain 1–20 characters of any type.

ID/Name/Tag	Anti-DDoS Adv	Specifications
bgpip-000002tb Unnamed 🖍 N/A 🖍	119.28.217.248	Line: BGP(Hong Kong, China) Application Bandwidth: 100Mbps Package type: Standard pack

Method 2

- 1. Log in to the new Anti-DDoS Advanced Console and click Instance List on the left sidebar.
- 2. In the instance list, click the ID in the "ID/Name/Tag" column of the target instance to enter the instance basic information page.

3. On the basic information page of the instance, click the "Modify" pencil icon on the right of the instance name and enter a name.

The name can contain 1–20 characters of any type.

Basic Information

Anti-DDoS Advanced Name	Unnamed 🎤
Location	Hong Kong, China
IP	119.28.217.248
Base Protection Bandwidth	50Gbps
CC Protection Peak	150000QPS
Line	BGP
Max forwarding rules	60

Configuring Intelligent Scheduling

Last updated : 2022-08-04 11:20:56

Use Cases

Each account can have multiple Anti-DDoS instances, and each instance has at least one protective line; therefore, there can be multiple protective lines under one account. Once your business is added to an Anti-DDoS instance, a protective line will be configured for it. If multiple protective lines have been configured, you need to choose the optimal business traffic scheduling method, i.e., how to schedule business traffic to the optimal line for protection while ensuring high business access speed and availability.

Anti-DDoS features priority-based CNAME intelligent scheduling, where you can select an Anti-DDoS instance and set the priority of its protective line as needed.

Note :

DNS configuration is supported for Anti-DDoS Pro instances and Anti-DDoS Advanced instances (including instances for BGP, China Telecom, China Unicom, and China Mobile).

Priority-based Scheduling

This refers to using the protective line of the highest priority to respond to all DNS requests, i.e., all access traffic will be scheduled to the protective line of the currently highest priority. You can adjust the priority value of a protective line, which is 100 by default. The smaller the value, the higher the priority. The specific scheduling rules are as follows:

- If the Anti-DDoS instance configured for your business contains multiple protective lines from different ISPs and of the same priority, response will be made based on the ISP of the specific DNS request. If one of the lines is blocked, access traffic will be scheduled in the order of BGP > China Telecom > China Unicom > China Mobile > ISPs outside Mainland China (including those in Hong Kong (China) and Taiwan (China)).
- If all the lines of the same priority are blocked, access traffic will be automatically scheduled to the currently available protective line of the second-highest priority.

Note :

If no protective lines of the second-highest priority are available, automatic scheduling cannot be completed, and business access will be interrupted.

• If the Anti-DDoS instance configured for your business contains multiple protective lines from the same ISP and of the same priority, access traffic will be scheduled by way of load balancing, i.e., evenly distributed to such lines.

Example

Suppose you have the following Anti-DDoS instances: BGP IPs 1.1.1.1 and 1.1.1.2 , China Telecom IP 2.2.2.2 , and China Unicom IP 3.3.3.3 , of which the priority of 1.1.1.2 is 2 and that of the rest is 1. Normally, all traffic will be scheduled to the protective lines with the current priority of 1. Specifically, traffic from China Unicom will be scheduled to 3.3.3.3 , that from China Telecom to 2.2.2.2 , and that from other ISPs to 1.1.1.1 . If 1.1.1.1 is blocked, access traffic under this IP will be automatically scheduled to 2.2.2.2 . If both 1.1.1.1 and 3.3.3.3 are blocked, traffic supposed to be scheduled to them will be distributed to 2.2.2.2 , and if 2.2.2.2 is blocked too, traffic will be scheduled to 1.1.1.2 .

Prerequisites

• Before enabling intelligent scheduling, please connect your business to be protected to your Anti-DDoS instance.

Note :

- If you need to add the IP of your protected Tencent Cloud service to a purchased Anti-DDoS Pro instance, please see Getting Started with Anti-DDoS Pro.
- If you need to connect your layer-4 or layer-7 application to a purchased Anti-DDoS Advanced instance,
 please see Anti-DDoS Advanced documents Port Connection or Domain Name Connection.
- To modify the DNS resolution, you need to purchase the domain name resolution product.

Setting Line Priority

Please follow the steps below to set priorities for your Anti-DDoS instance based on your scheduling scheme:

1. Log in to the new Anti-DDoS Advanced Console and click **Intelligent Scheduling** on the left sidebar to enter the list page. Click **Add Scheduling**, and the system will automatically generate a CNAME record.



Smar	t Scheduling						Purchase
	New Scheduling Policy					CNAME	Q
	CNAME	Parsing Status	Associated IP	Scheduling Mode	Last Modified Time	Operation	
	j6z1mo4q.dayugslb.com	Not running	Add Anti-DDoS instance	Priority	2020-07-01 09:52:31	Configuration Delete	
	v3drws2b.dayugslb.com	Not running	Add Anti-DDoS instance	Priority	2020-07-01 09:52:29	Configuration Delete	

2. Locate the row of the CNAME record and click **Add Anti-DDoS Instance** to enter the intelligent scheduling editing page.

Smart Scheduling						Purchase
New Scheduling Policy					CNAME Please enter the co	Q
CNAME	Parsing Status	Associated IP	Scheduling Mode	Last Modified Time	Operation	
j6z1mo4q.dayugslb.com	Not running	Add Anti-DDoS instance	Priority	2020-07-01 09:52:31	Configuration Delete	
v3drws2b.dayugslb.com	Not running	Add Anti-DDoS instance	Priority	2020-07-01 09:52:29	Configuration Delete	
qo0in9hm.dayugslb.com	Running	2 associated IPs (j)	Priority	2020-06-30 21:21:51	Configuration Delete	

3. On the intelligent scheduling editing page, the TTL value is 60s by default, which can range from 1s to 3,600s, and the default scheduling method is priority-based.







4. Click Add Anti-DDoS Resource IP, select the target Anti-DDoS Advanced instance and IP, and click OK.

elect resource type	Anti-DDoS Advance	•					
elect resource	Service Packs				Selected (0)		
	Anti-DDoS Advance		Q		Resource ID/Na	IP Address	Resource Type
Resource ID/Na	me IP Address	Res	ource Type				
bgpip-000002td	188.131.208.27	Anti	-DDoS Advance				
bgpip-000002tb	119.28.217.248	Anti	-DDoS Advance				
bgpip-000002ta	117.184.254.232	Anti	-DDoS Advance	\leftrightarrow			
bgpip-000002t9	153.3.137.208	Anti	-DDoS Advance				
bgpip-000002t8	183.131.196.215	Anti	-DDoS Advance				
bgpip-000002rr	119.28.217.239	Anti	-DDoS Advance				

5. After the instance is selected, domain name resolution will be enabled for its protective line by default. At this point, you can set the line priority.

CNAME	j6z1mo4q.dayugslb.	com					
TTL Value	60 seconds 🧪						
Mode	O Priority						
Associated IP	Add Anti-DDoS IP Ad	dd non-Anti-DDoS) IP				
	IP	Priority	Line	Region	Status	Domain Name	Operation
	119.28.217.248 (bgpip-000002tb)	100 🎤	Outside Mainland China	Hong Kong, China	Running		Unbind
	2402:4e00:1400:e 57b:0:8f9c:903:5e 6e	100 🔊	BGP	Shanghai	Running		Unbind

Example

Suppose you want to implement the following scheme: the business traffic will be scheduled to a BGP protective line first; if it is blocked due to attacks, the traffic will be automatically scheduled to a China Telecom protective line; if it is also blocked, the traffic will be scheduled to a China Unicom protective line; and after the BGP protective line is unblocked, the traffic will be scheduled to it automatically.

To implement this scheduling scheme, set the priority of the BGP line in the Anti-DDoS instance to 1 and that of the China Telecom line to 2, and keep the priority of the China Unicom line unchanged.

IP	Priority	Line	Region	Status	Domain Name	Operation
183.131.196.215 (bgpip-000002t8)	100 🖍	СТСС	Hangzhou	Running		Unbind
153.3.137.208 (bgpip-000002t9)	100 🖍	CUCC	Nanjing	Running		Unbind
2402:4e00:1400:e 57b:0:8f9c:903:5e 6e (bgp-000000cm)	100 🎤	BGP	Shanghai	Running		Unbind

If you do not want the China Unicom protective line to be in the traffic scheduling scheme, click when necessary.

If you want to delete it from the current scheduling scheme, you can locate the row of its corresponding instance and click **Unbind**.

Modifying DNS Resolution

Before using a CNAME record for intelligent scheduling, you are recommended to change the CNAME record of your business domain name DNS to the CNAME record automatically generated by the intelligent scheduling system of Tencent Cloud Anti-DDoS, to which all access traffic to your business website will be directed.

Setting Security Event Notification

Last updated : 2020-07-07 17:19:18

Alarm messages for Anti-DDoS Advanced will be sent to you through Message Center, SMS, or email in the following conditions (the receipt methods configured on the Message Center Subscription page shall prevail):

- An attack starts.
- An attack ended 15 minutes ago.
- An IP is blocked.
- An IP is unblocked.

You can modify the recipients and how they receive the alarm messages as needed.

Setting Alarm Threshold

- 1. Log in to the new Anti-DDoS Advanced Console and select Alarm Notification on the left sidebar.
- 2. You can set the "inbound traffic alarm threshold for single IP" and "DDoS cleansing threshold" in the feature blocks on the right.

Inbound Traffic Thresho	ld Per IP	DDoS Cleansing Traffic Alarm				
When the inbound traffic to a notification in the message ca	n IP exceeds the threshold, you will get enter.	When an IP is being attack, and the inbound traffic exceeds the three cleansing is triggered, and you will get notifications in message center				
Advanced Settings	Default threshold: 200 Mbps 🧪	Advanced Settings	Default threshold: 200 Mbps 🧪			

3. Click the pencil icon on the right of the default threshold for one single IP to modify the default threshold. After the modification is completed, click **OK**.

Modify Threshol	d	×
Set Threshold	— 200 + Mbps	
	OK Cancel	

- 4. Click **Advanced Settings** in a block to enter the IP alarm settings list, where you can set different alarm thresholds for different IPs.
 - Inbound traffic alarm for single IP

÷	Inbound Traffic Threshold Per IP					
	Batch Modify				Enter the IP to be q	Q
	Resource Instance	Bound IP	Inbound traffic alarm threshold (Mbps)	Operation		
	bgpip-000002td	188.131.208.27	200	Modify		
	bgpip-000002tb	119.28.217.248	200	Modify		

• DDoS cleansing threshold

÷	DDoS Cleansing Alarm					
	Batch Modify				Enter the IP to be q	Q
	Resource Instance	Bound IP	DDoS Cleansing Threshold (Mbps)	Operation		
	bgpip-000002td	188.131.208.27	200	Modify		
	bgpip-000002tb	119.28.217.248	200	Modify		

Setting Notification Method

1. Log in to your Tencent Cloud account and go to the Message Center.

Alternatively, you can log in to the console, click in the top-right corner, and then click View More in the pop-up window to enter the Message Center.

- 2. Click Message Subscription on the left sidebar to enter the message list.
- 3. In the message list, select the receipt methods on the row of Security Event Notification and click Modify

Message Recipient to enter the message recipient modifying page.

 Security notifications 				
Attack notifications	~	~	8163196@qq.com	Modify Message Receiver
Illegal Contents Notifications	~		8163196@qq.com	Modify Message Receiver

4. On the message recipient modifying page, set the message recipients. After completing the settings, click OK.

Modify Messa	ge Receiver					
i Please	make sure that the user's e	mail and mobile are verified by Tencent Cloud, an	d the responding method is enabled.			
lessage Type	Attack notifications					
ecipients	User User Gro	up Add Messag	e Receiver 🖆 Modify User Information 본		1 selected	
	Search for user name		Q		8163196@qq.com	×
	- User Name	Mobile Number	Email			
	✓ 8163196@qq.com	⊘ 158****0375	1 81*****@qq.com			
	v_szgwu	⊘ 188****5245	⊘ v_*****@tencent.com			
				\Leftrightarrow		
			OK Cancel			

Viewing Operation Log

Last updated : 2020-07-07 17:19:18

Operation Scenarios

Anti-DDoS Advanced allows you to view logs of important operations in the last 90 days in the console. The following types of logs are available:

- Logs of forwarding rule change
- · Logs of protection policy change
- · Logs of cleansing threshold adjustment
- Logs of protection level change
- Logs of instance name change

Directions

- 1. Log in to the new Anti-DDoS Advanced Console and click **Operation Log** on the left sidebar.
- On the operation log page, you can query operation logs by time period. You can click **Show More** in the "Operation" column on the right to view log details.

Today Yesterday	Last 7 days Last 30 days	2020-06-06 00:00 ~ 2020-07-0	6 23:59			
Operation Time	Object ID	Product Type	Action	Result	Operator Account	Operation
2020-07-03 17:07:34	2687	Anti-DDoS Advance	Add layer-7 forwarding rule	Success	100001500880	Unfold
2020-07-03 17:07:07	2687	Anti-DDoS Advance	Delete layer-7 forwarding rule	Success	100001500880	Unfold
2020-07-03 17:06:30	2970	Anti-DDoS Advance	Delete layer-7 forwarding rule	Success	100001500880	Unfold

Blocking Operations Connecting a Blocked Server

Last updated : 2023-04-28 16:51:55

This document describes how to connect a blocked server.

Directions

- 1. Log in to the CVM Console and click Instances on the left sidebar.
- 2. Click the drop-down list in the top left corner and modify the region.
- 3. Click the search box to use filters such as "Instance Name", "Instance ID" and "Instance Status" to locate the blocked server.
- 4. Click Log In for the blocked server to display the Log in to Linux Instance pop-up window.
- 5. In the pop-up window, select Login over VNC and click Log In Now to connect the server via browser VNC.

Unblocking an IP

Last updated : 2022-11-23 10:55:46

Unblocking Procedure

Auto unblocking

With auto unblocking, you only need to wait until blocked IPs are unblocked automatically. You can check the predicted unblocking time as follows:

- Log in to the Anti-DDoS console. Select Self-Service Unblocking > Unblock Blocked IP on the left sidebar to get to unblocking operation.
- 2. Check the predicted unblocking time of the IP in Estimated Unblocking Time on the unblocking page.

Chances for self-service unblocking

Only three chances of self-service unblocking are provided for Anti-DDoS Advanced every day. The system resets the chance counter daily at midnight. Unused chances cannot be accumulated for the next day.

Note :

- The unblocking may fail for risk management reasons. A failed attempt does not count as a chance. Please wait for a while and then try again.
- Before unblocking the IP, please check the predicted unblocking time which may be affected by some factors and will be postponed. If you accept the predicted time, you do not need to operate manually.
- If the self-recovery chances are used up for the day, you can upgrade the base protection capability or the elastic protection capability to defend against large traffic attack and avoid continuous blocking.

Manual unblocking

 Log in to the Anti-DDoS console. Select Self-Service Unblocking > Unblock Blocked IP on the left sidebar to get to unblocking operation. 2. Find the protected IP in **Pending Auto Unblocking** and click **Unblock** in the **Operation** column on the right.

Anti-DDoS	Unblocking Operation					
Cverview	Total Quotas		Currently used		Not currently used	
Anti-DDoS Basic	3		0		3	
Anti-DDoS ~ Advanced	-		-		-	
다 Anti-DDoS Pro 🗸	IP	Defense Status	Blocking time	Estimated unblocking time	Status	Operation
Intelligent Scheduling Policy		Anti-DDoS	2022-11-15 17:00:00	2022-11-16 16:55:00	Automatically unbicoking	Unblock
Anti-DDoS Pro (New)						
Anti-DDoS ~ Advanced (New)						
🖻 Edge Defender 🛛 👻						
Manual ^ Unblocking						
Unblocking Operation						
Unblocking Log						

3. Click **OK** in the **Unblock Blocked IP** dialog box. If you receive a notification indicating successful unblocking, the IP has been successfully unblocked. You can refresh the page to check whether the protected IP is in running status.

Unblocking Operation Record

Log in to the Anti-DDoS console. Select **Self-Service Unblocking** > **Unblocking History** on the left sidebar. You can check all unblocking records in the specified period, including records of automatic and manual unblocking.

Unblocking Log			
2022-08-15 17:14:11 ~ 2022-11-15 17:14:11			
lb	Blocking time	Actual unblocking time	Unblocking operation type
	2022-11-15 17:00:00	2022-11-15 17:01:00	Automatically unblock
	2022-10-28 15:35:00	2022-10-28 16:48:58	Self-service unblocking
	2022-10-28 15:30:00	2022-10-28 16:39-29	Self-service unblocking
	2022-10-27 15:30:00	2022-10-28 16:16:58	Automatically unblock
	2022-10-13 14:25:00	2022-10-13 14:28:00	Automatically unblock
	2022-10-13 14:15:00	2022-10-13 14:18:00	Automatically unblock
	2022-10-13 10:58:00	2022-10-13 11:00:00	Automatically unblock
	2022-10-13 10:50:00	2022-10-13 10:52:00	Automatically unblock